



Les cryptomonnaies et les enquêtes sur le blanchiment de capitaux



Federico Paesano

Spécialiste en enquêtes financières senior

Jusqu'à présent, ce fut un voyage incroyable. J'ai entendu parler du bitcoin pour la première fois en 2010, lors d'une conférence sur la cybercriminalité. Nous ne savions pas encore grand-chose, si ce n'est qu'il s'agissait d'une nouvelle forme d'argent, totalement décentralisée puisqu'elle n'était ni émise ni contrôlée par un gouvernement, et qu'elle pouvait potentiellement aider les criminels à déplacer et à blanchir leurs revenus au-delà des frontières sans être détectés.

Comment l'argent peut-il être décentralisé ? Les criminels peuvent-ils convertir leurs fonds mal acquis en bitcoins, puis en monnaie fiduciaire ? Si l'adoption du bitcoin croît de manière exponentielle, les forces de l'ordre n'ont-elles plus rien à craindre ? Telles étaient nos questions à l'époque.

La réponse à la dernière question semblait être un grand « oui », car les activités criminelles dans ce domaine avaient commencé à être détectées et il semblait encore impossible d'enquêter sur les flux de crypto-monnaies sur la blockchain. L'utilisation du bitcoin apparaissait comme l'outil ultime de l'anonymat.

Une attention croissante

Lorsque le Basel Institute on Governance a décidé de s'asseoir avec Europol, INTERPOL et un autre petit groupe d'enquêteurs de différentes parties du monde, ce sujet occupait un créneau minuscule.

À peu de choses près, il n'y avait que nous, à savoir les 20 personnes partageant une petite salle de l'Université de Bâle, une seule cryptomonnaie (le Bitcoin) et un seul dossier à commenter (l'affaire Silk Road). Nous avons tout de même décidé de cofonder un Groupe de Travail sur les cryptomonnaies et le blanchiment d'argent. Nous pouvions sentir que quelque chose d'énorme était en train de bouger, et que les forces de l'ordre devaient être prêtes à relever ce défi.

Mais quel changement en quelques années ! Aujourd'hui, des milliers de personnes demandent à assister à notre Conférence Mondiale annuelle sur le Financement du Crime et les Cryptomonnaies. Il existe des centaines de nouvelles cryptomonnaies et d'autres formes innovantes d'actifs virtuels, comme les jetons non fongibles, ainsi qu'un nombre croissant d'affaires de blanchiment d'argent contraignant les enquêteurs à pénétrer la « cryptosphère ».

Les régulateurs internationaux prennent également le sujet plus au sérieux. Le Groupe d'action financière (GAFI), qui intervient en tant qu'instance mondiale de lutte contre le blanchiment d'argent, a énoncé une version mise à jour des normes et lignes directrices sur les actifs virtuels et les prestataires de services d'actifs virtuels (PSAV), et assure étroitement le suivi des progrès réalisés par les pays en matière de conformité.

Et en juin 2023, l'Union européenne a adopté le cadre réglementaire le plus complet à ce jour pour les actifs numériques : le Règlement sur les Marchés des Crypto-actifs (MiCA).

Quels sont les types d'infractions en lien avec des cryptomonnaies ?

Les cryptomonnaies donnent lieu à un grand nombre d'usages et d'avantages légitimes, qui incluent leur potentiel de mise à disposition d'un système de paiement à bas prix, rapide, accessible et international à des millions de personnes du monde entier ne bénéficiant pas de services bancaires. Cependant, comme toute réserve de valeur, elle peut faire l'objet d'usages impropres.

Certains cas concernent des criminels ayant recours à des cryptomonnaies pour blanchir les produits « normaux » du crime ou de la corruption. Un exemple simple est celui d'un fonctionnaire corrompu recevant des pots-de-vin et s'efforçant de dissimuler l'origine de l'argent en réalisant une multitude de transferts de fonds entre diverses cryptomonnaies et monnaies fiduciaires, comme le dollar.

Cependant, dans la plupart des cas, le thème dont nous traitons est celui des infractions dégageant des bénéfices en cryptomonnaie. Comme le décrit l'Internet Organised Crime Threat Assessment (Évaluation de la menace que représente le crime organisé en ligne) d'Europol, les cryptomonnaies sont utilisées pour faciliter les paiements liés à diverses formes d'activités illicites.

Elles englobent le commerce de stupéfiants et d'autres marchandises illégales sur le dark web, les logiciels d'extorsion comme Rhysida ou Abyss Locker, les paiements en lien avec les enlèvements et les rançons, et la cybercriminalité.

Le traçage de l'argent virtuel - une opération plus facile dans certains cas, et plus difficile dans d'autres cas

La blockchain, la technologie derrière les cryptomonnaies, facilite théoriquement la tâche des enquêteurs financiers "suivant la trace de l'argent". Pourquoi ? Parce que chaque opération est définitivement saisie dans un registre partagé, la blockchain, et ne pouvant pas être modifiée ou falsifiée par la suite. Théoriquement, la trace de l'argent y restera à jamais, et peut devenir une preuve même des années plus tard.

La récente poursuite contre un individu qui avait volé plus de 50 000 bitcoins à la défunte bourse de crypto-monnaies MtGox en 2012 illustrent clairement ce processus. L'immuabilité de la blockchain a permis aux forces de l'ordre de suivre l'argent, d'identifier l'auteur du vol et de récupérer un montant record de 3,36 milliards USD d'actifs, près de 10 ans après les faits.

La situation n'est pas la même pour les opérations en espèces, par exemple. Il est en effet impossible de remonter le temps et de découvrir les parties à une opération et son objet.

Les transactions en Bitcoin donnent l'heure et le montant de l'opération, ainsi que les adresses de l'expéditeur et du destinataire (des pseudonymes se présentant comme de longues chaînes de caractères alphanumériques). En revanche, les cryptomonnaies plus petites et davantage axées sur la confidentialité, comme Monero, cachent ces informations.

La difficulté de toutes ces affaires est *l'imputabilité* : l'établissement d'un lien entre, d'une part, des opérations et des adresses et, d'autre part, des personnes physiques du monde réel. Autrement dit, l'identification des opérations potentiellement criminelles ainsi que des criminels les ayant conclues.

Percer le bouclier de l'anonymat

Fort heureusement pour les enquêteurs, il existe des techniques permettant de lever l'anonymat apparent des cryptomonnaies, et d'associer des opérations et des adresses à des personnes soupçonnées d'avoir commis des infractions et blanchi de l'argent.

Par exemple, des heuristiques peuvent être utilisées pour créer des clusters, c'est-à-dire des groupes d'adresses susceptibles d'être contrôlés par une seule et même entité. Des techniques spéciales sont ensuite utilisées pour supprimer l'anonymat de ces clusters.

Il s'agit du stade auquel les sociétés d'analyse blockchain peuvent intervenir. Elles peuvent procéder, moyennant un paiement, à l'analyse des adresses et des opérations pour obtenir des informations cruciales, comme les données de géolocalisation ou la plateforme d'échange ayant été utilisée pour acheter des cryptomonnaies.

Les enquêteurs peuvent ensuite adresser à la plateforme d'échange une demande d'informations supplémentaires, tout comme ils le feraient dans leurs relations avec une banque ou un autre prestataire de services de paiement. Dans la mesure où les normes du GAFI mentionnées ci-dessus et relatives aux PSAV sont déployées par l'intermédiaire d'une législation nationale, nous espérons et voulons que des données plus fiables sur leurs clients soient placées à la disposition des autorités compétentes.

Les frais de consultation d'une société d'analyse blockchain pourraient constituer un obstacle dans les pays où les ressources affectées aux forces de l'ordre sont limitées.

Cependant, la plupart des enquêtes impliquant les cryptomonnaies débutent en fait avec un suspect, et non pas avec une opération douteuse ou une adresse anonyme. Les enquêteurs cherchent simplement à identifier les adresses de cryptomonnaie dont un suspect a le contrôle. Ces informations peuvent souvent être révélées par une analyse scientifique des appareils du suspect, sans que la consultation d'une société d'analyse blockchain ne s'impose.

L'engagement de poursuites dans une affaire ; pourquoi les témoins experts sont-ils utiles ?

En raison de la nature récente et rapidement évolutive des actifs virtuels, les technologies blockchain, comme les cryptomonnaies, sont communément incomprises.

Le problème se pose pour les agents des forces de l'ordre et les auxiliaires de justice, qui pourraient avoir à interpréter les preuves dévoilées par une analyse blockchain ou des portefeuilles numériques pour que la culpabilité d'un suspect soit reconnue.

Dans ce cas, il est utile de faire appel à un témoin expert chargé de donner des éclaircissements sur ces preuves et de les confirmer devant un tribunal. Bien entendu, une explication claire sur les étapes suivies lors de l'enquête jouera également un rôle dans la démonstration à la cour du fait que les preuves obtenues sont tout simplement similaires à toute autre preuve d'une infraction financière.

Le recouvrement des avoirs volés et détenus en cryptomonnaies

Les avoirs détenus en cryptomonnaies peuvent être traités comme des avoirs conservés sur des comptes bancaires ou faisant partie d'un bien immobilier. Par exemple, un juge peut prononcer une ordonnance de gel des avoirs visant un compte de cryptomonnaie, en attendant l'issue d'une affaire.

Cependant, étant donné que les opérations en cryptomonnaies peuvent être effectuées en quelques minutes, la coopération internationale en matière de gel des avoirs doit réellement accélérer. Même pour les virements bancaires usuels, dans le délai nécessaire au prononcé d'une ordonnance de gel, les fonds concernés peuvent avoir fait plusieurs fois le tour de la planète.

S'agissant de la confiscation et du recouvrement des avoirs détenus en cryptomonnaies, les pouvoirs publics, qui utilisent encore les monnaies fiduciaires nationales, encore que nul ne sait ce que l'avenir nous réserve, ont deux possibilités.

- La première consiste à utiliser la plateforme d'échange pour convertir la cryptomonnaie dans la monnaie fiduciaire souhaitée.
- La deuxième consiste à réaliser une vente aux enchères. En 2013, le Département de la Justice des États-Unis a récupéré presque 50 millions USD en vendant aux enchères un magot de bitcoins illicites suite à la clôture du marché en ligne « Silk Road ».

Pour les personnes tenues de recouvrer des avoirs, la volatilité du cours des cryptomonnaies est un casse-tête. Si les ventes aux enchères relevant de l'affaire Silk Road et tenues pour 144 336 bitcoins avaient lieu aujourd'hui, elles auraient dégagé près de 4.2 milliards USD.

Que peuvent faire les forces de l'ordre ?

Lors de la 6e Conférence mondiale sur les crypto-monnaies et les finances criminelles en 2022, organisée conjointement par l'Institut de Bâle et Europol et à laquelle ont assisté plus de 2 000 participants en personne et à distance, cing recommandations ont émergé des discussions.

- 1. Casser les silos entre « traditionnel » et « crypto »** – ne pas traiter les crypto-monnaies comme un domaine séparé, mais opérer à travers les domaines physiques et virtuels (comme le font les criminels).
- 2. Réglementer largement et utiliser pleinement les lois existantes** – pour s'assurer que les crypto-actifs sont traités comme n'importe quel autre actif aux fins de la surveillance, de l'application et du recouvrement des actifs dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

3. Tirer parti de la blockchain pour perturber la criminalité organisée

– étant donné que la blockchain offre de nombreuses possibilités d'enquêter sur la criminalité et les systèmes de blanchiment d'argent et de les perturber, de recueillir des renseignements et de geler et confisquer les actifs illicites.

4. Améliorer la connaissance des crypto-monnaies par le renforcement des capacités et une communication claire

– en éliminant le jargon et les acronymes et en étendant la formation de base à des groupes de personnel plus larges.

5. Accroître la coopération public-privé

– car les services répressifs peuvent tirer profit des compétences techniques des sociétés d'analyse de la blockchain et de traçage des actifs, et coopérer avec les fournisseurs de services de crypto-actifs pour accélérer les ordres de gel et le partage d'informations.



Publié originellement en anglais le 15 mars 2019 et mis à jour le 11 août 2023.
Tous nos guides rapides sont disponibles sur learn.baselgovernance.org

ISSN 2673-5229

Cette oeuvre est sous licence Creative Commons Attribution-Non commercial-NoDerivs 4.0 International License (CC BY-NC-ND 4.0).

